OIPE
JUN 2 4 2005
PATENT & TRADEMARK OFFICE

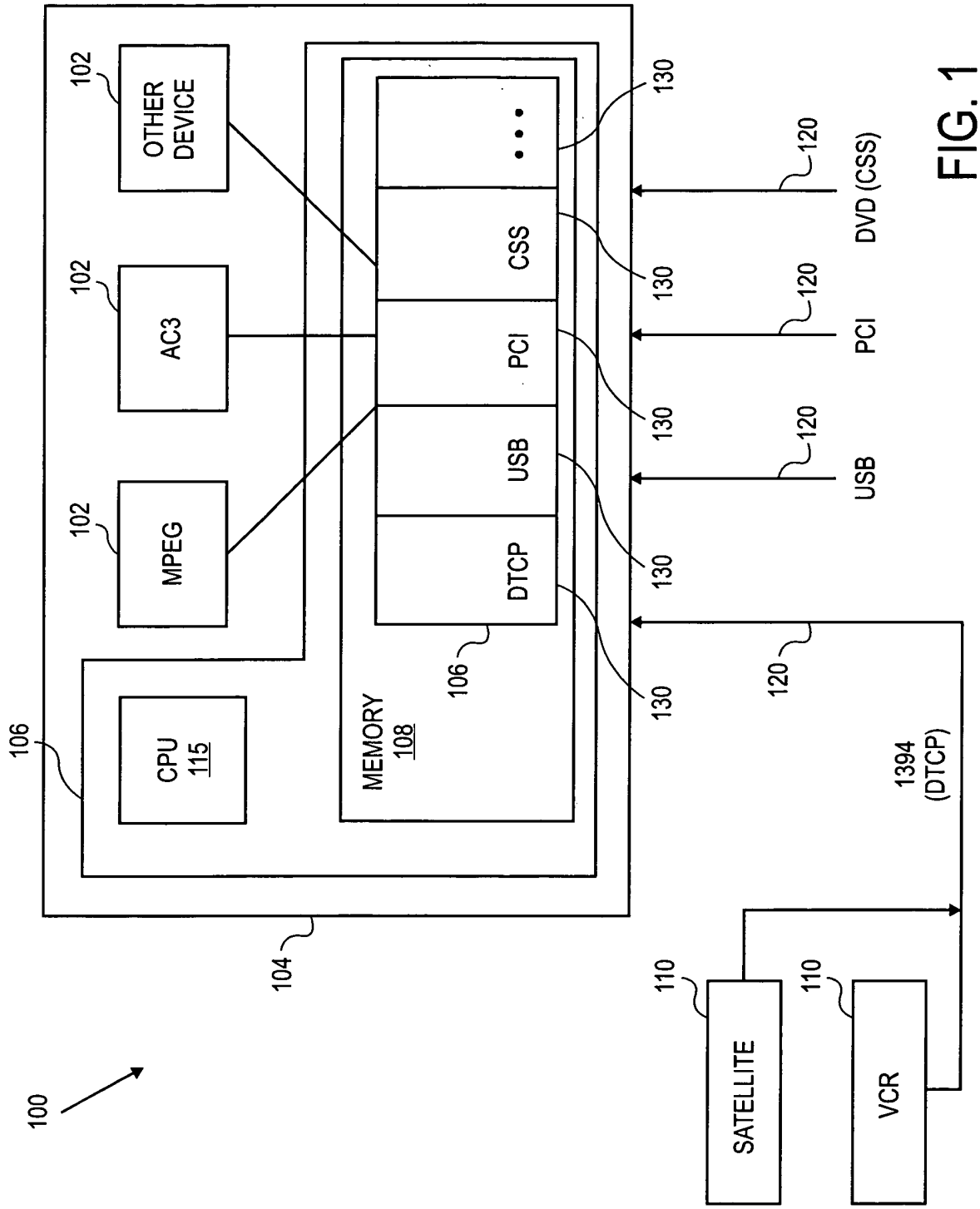


FIG. 1

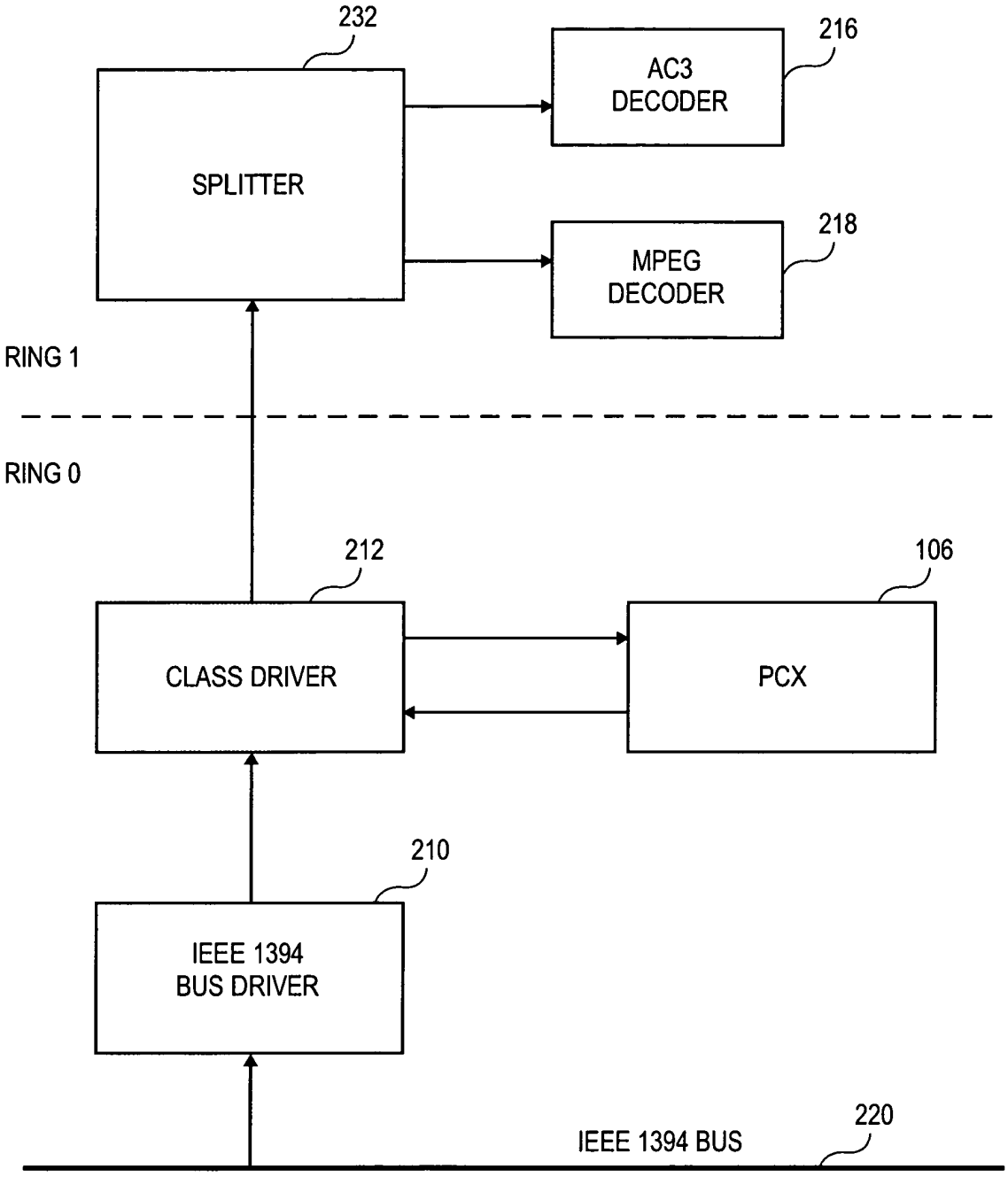

232
216
AC3
DECODER
SPLITTER
218
MPEG
DECODER
RING 1
RING 0
212
106
CLASS DRIVER
PCX
210
IEEE 1394
BUS DRIVER
220
IEEE 1394 BUS

FIG. 2

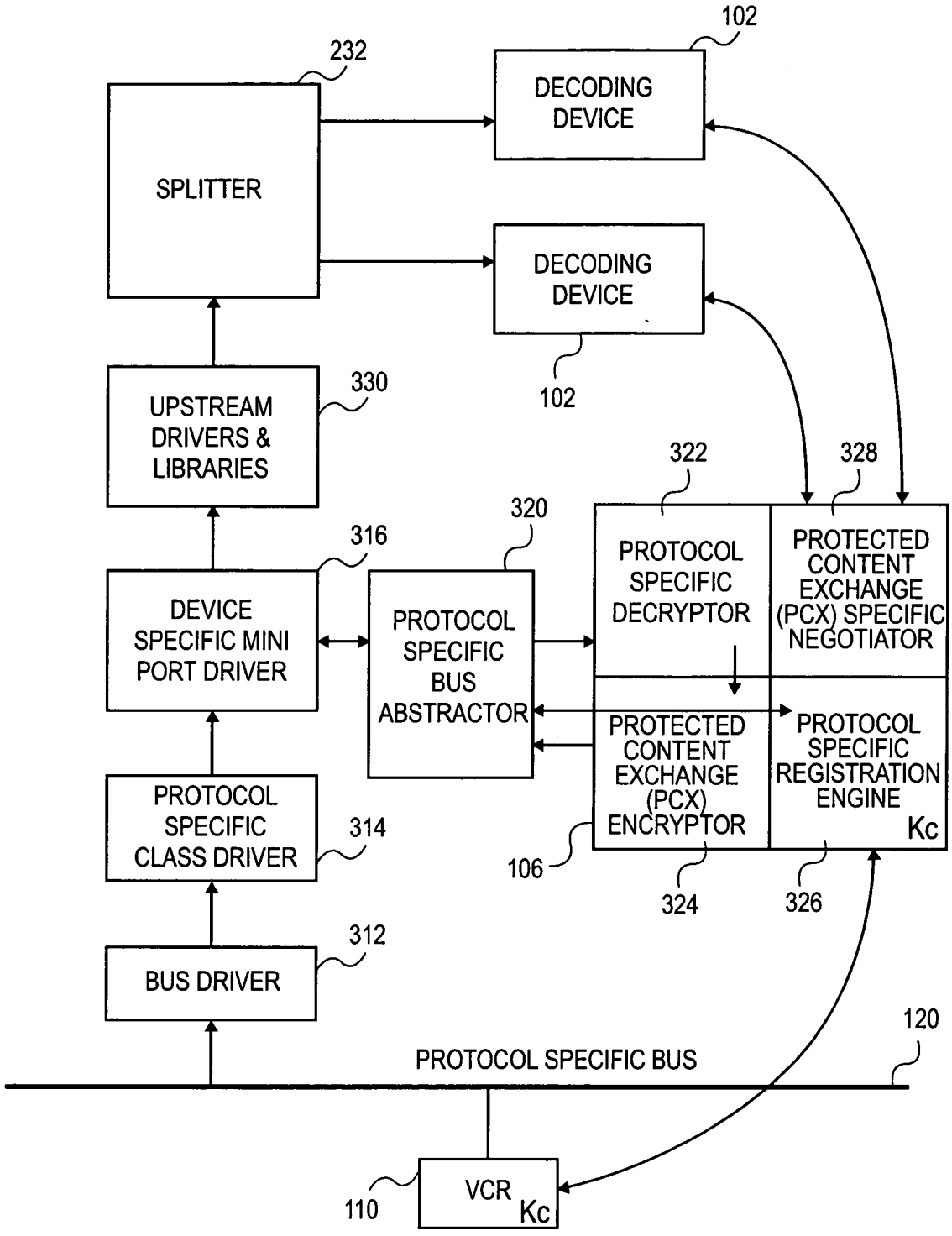

102
232
DECODING DEVICE
SPLITTER
DECODING DEVICE
102
330
UPSTREAM DRIVERS & LIBRARIES
322
328
320
316
PROTOCOL SPECIFIC DECRYPTOR
PROTECTED CONTENT EXCHANGE (PCX) SPECIFIC NEGOTIATOR
DEVICE SPECIFIC MINI PORT DRIVER
PROTOCOL SPECIFIC BUS ABSTRACTOR
PROTECTED CONTENT EXCHANGE (PCX) ENCRYPTOR
PROTOCOL SPECIFIC REGISTRATION ENGINE
Kc
106
324
326
PROTOCOL SPECIFIC CLASS DRIVER
314
312
BUS DRIVER
120
PROTOCOL SPECIFIC BUS
110
VCR
Kc

FIG. 3

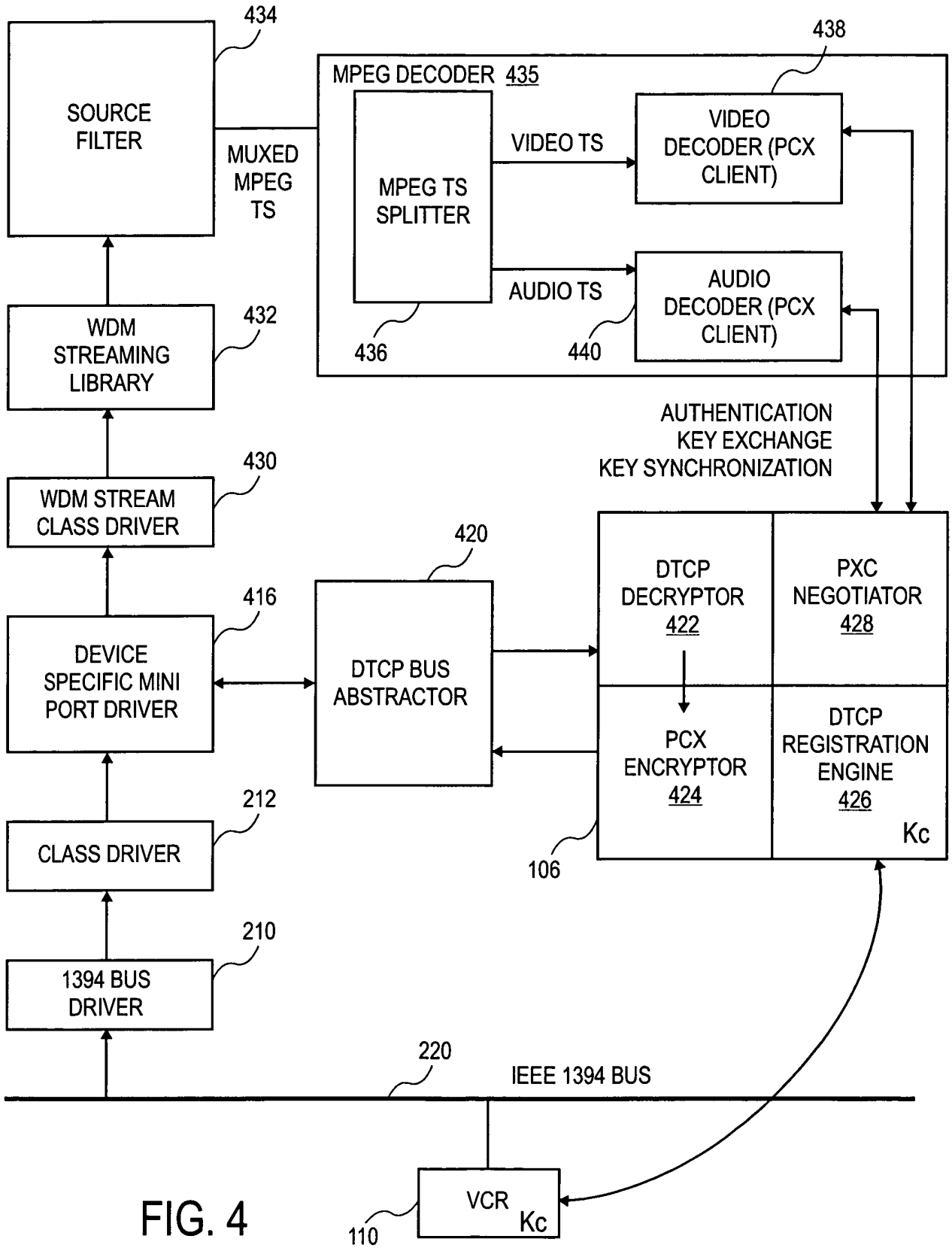

434
SOURCE FILTER
MUXED MPEG TS
438
MPEG DECODER 435
MPEG TS SPLITTER
VIDEO TS
VIDEO DECODER (PCX CLIENT)
AUDIO TS
AUDIO DECODER (PCX CLIENT)
436
440
WDM STREAMING LIBRARY
432
AUTHENTICATION
KEY EXCHANGE
KEY SYNCHRONIZATION
WDM STREAM CLASS DRIVER
430
420
DTCP DECRYPTOR 422
PXC NEGOTIATOR 428
416
DEVICE SPECIFIC MINI PORT DRIVER
DTCP BUS ABSTRACTOR
PCX ENCRYPTOR 424
DTCP REGISTRATION ENGINE 426
Kc
106
212
CLASS DRIVER
210
1394 BUS DRIVER
220
IEEE 1394 BUS
VCR Kc
110

FIG. 4

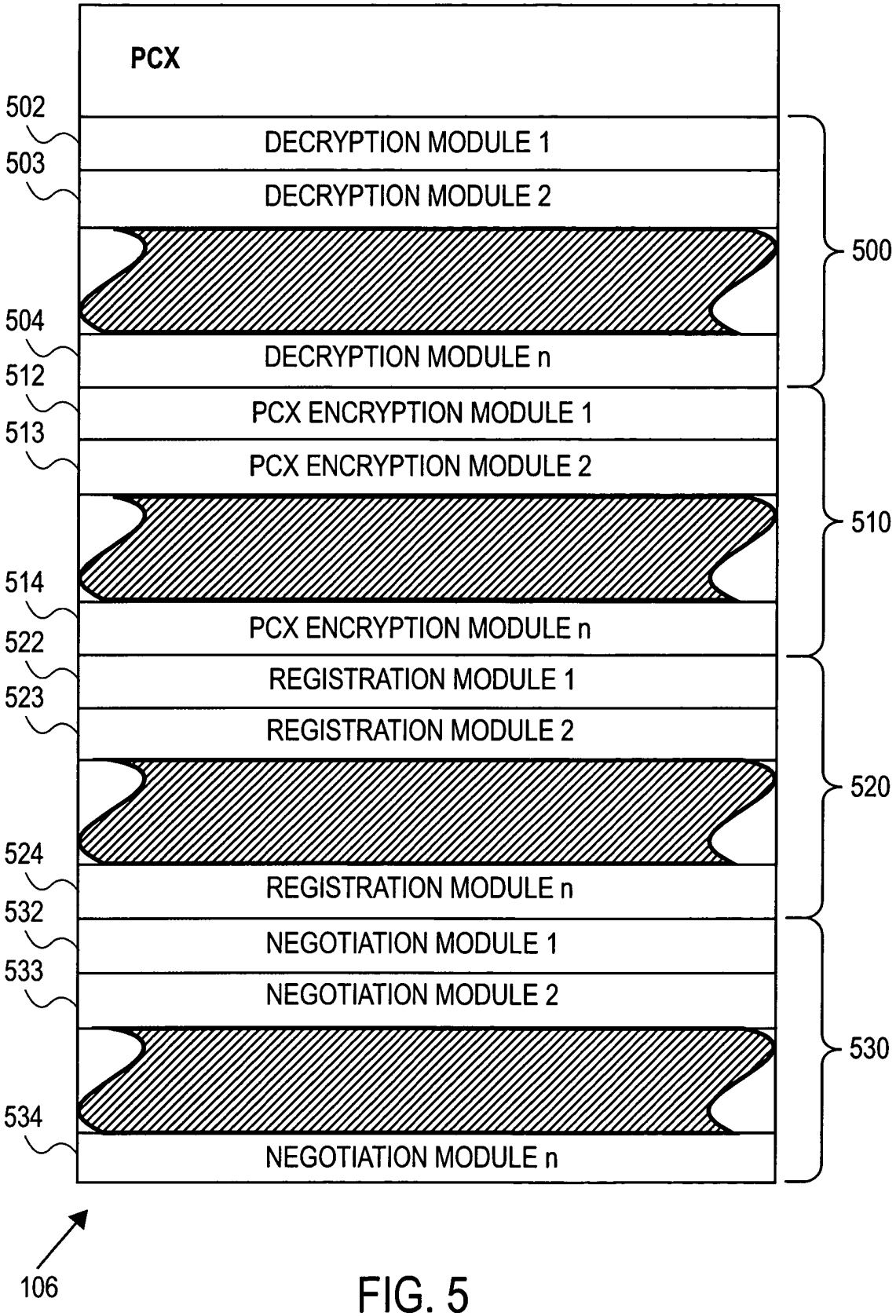

PCX
502
DECRYPTION MODULE 1
503
DECRYPTION MODULE 2
504
DECRYPTION MODULE n
500
512
PCX ENCRYPTION MODULE 1
513
PCX ENCRYPTION MODULE 2
514
PCX ENCRYPTION MODULE n
510
522
REGISTRATION MODULE 1
523
REGISTRATION MODULE 2
524
REGISTRATION MODULE n
520
532
NEGOTIATION MODULE 1
533
NEGOTIATION MODULE 2
534
NEGOTIATION MODULE n
530
106

FIG. 5

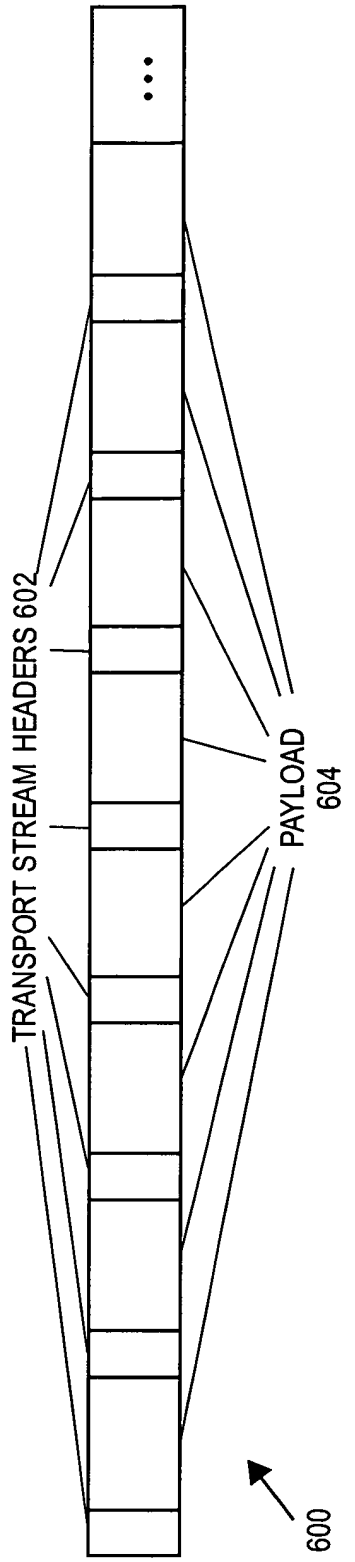

TRANSPORT STREAM HEADERS 602
PAYLOAD 604
600

FIG. 6A

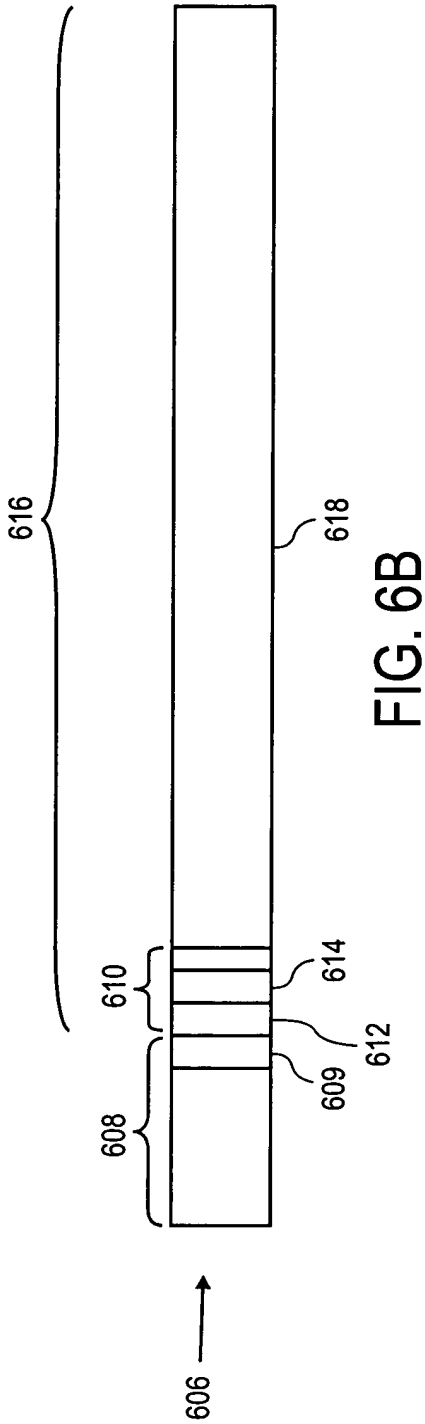

616
618
610
614
612
609
608
606

FIG. 6B

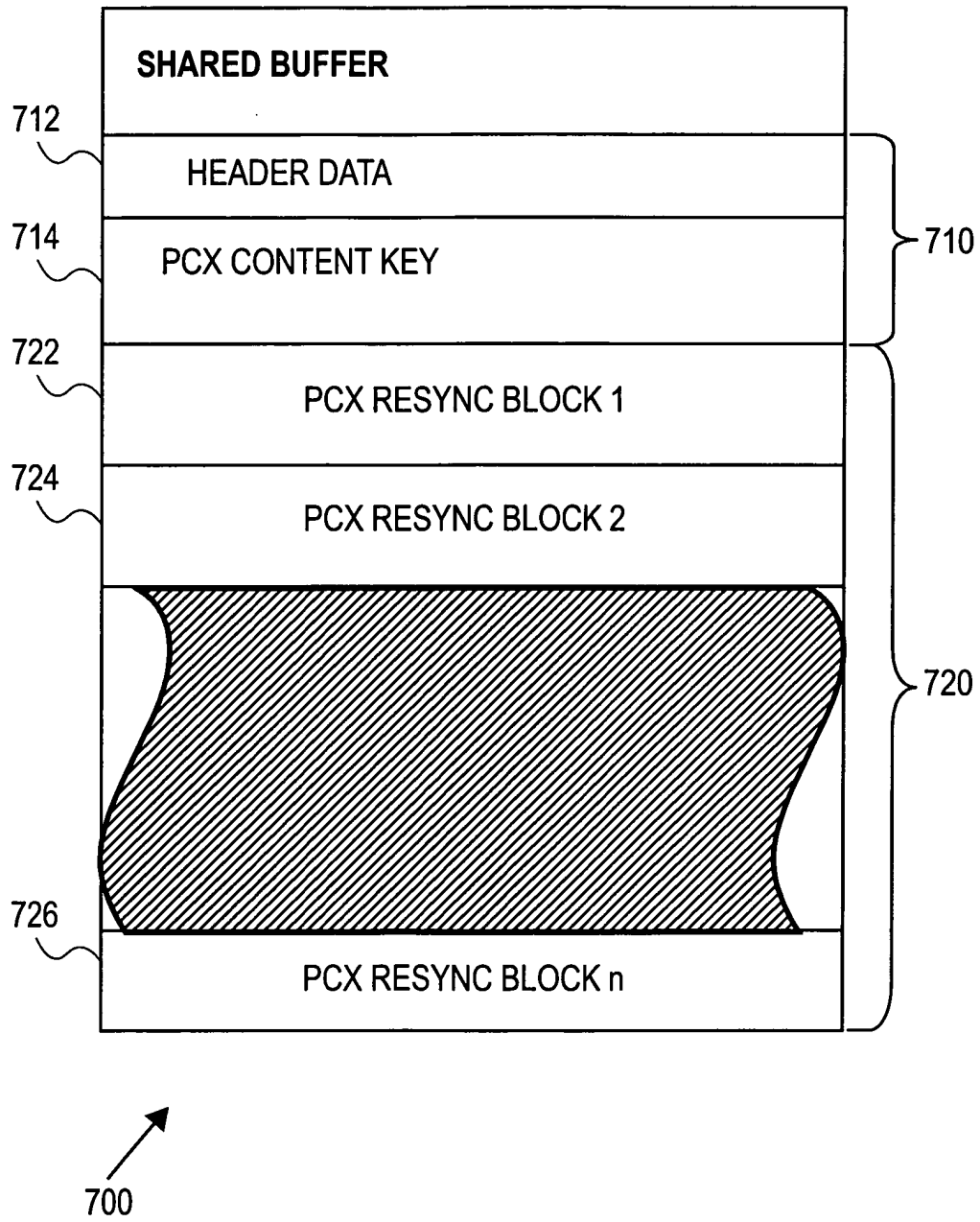
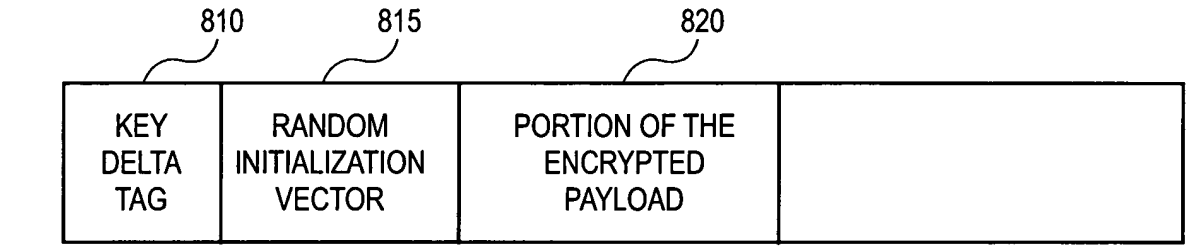

SHARED BUFFER
712
HEADER DATA
714
PCX CONTENT KEY
710
722
PCX RESYNC BLOCK 1
724
PCX RESYNC BLOCK 2
720
726
PCX RESYNC BLOCK n
700

FIG. 7


810
815
820
KEY DELTA TAG
RANDOM INITIALIZATION VECTOR
PORTION OF THE ENCRYPTED PAYLOAD

720

FIG. 8

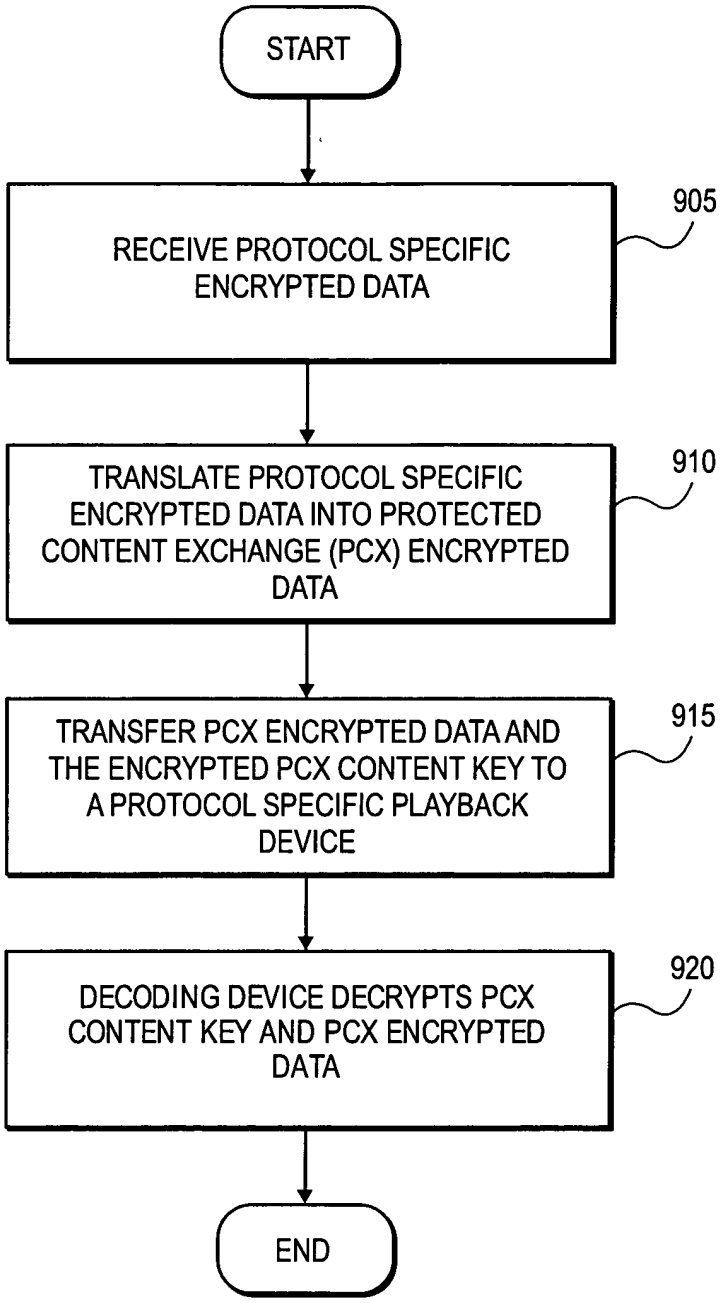

START
RECEIVE PROTOCOL SPECIFIC ENCRYPTED DATA
905
TRANSLATE PROTOCOL SPECIFIC ENCRYPTED DATA INTO PROTECTED CONTENT EXCHANGE (PCX) ENCRYPTED DATA
910
TRANSFER PCX ENCRYPTED DATA AND THE ENCRYPTED PCX CONTENT KEY TO A PROTOCOL SPECIFIC PLAYBACK DEVICE
915
DECODING DEVICE DECRYPTS PCX CONTENT KEY AND PCX ENCRYPTED DATA
920
END

FIG. 9

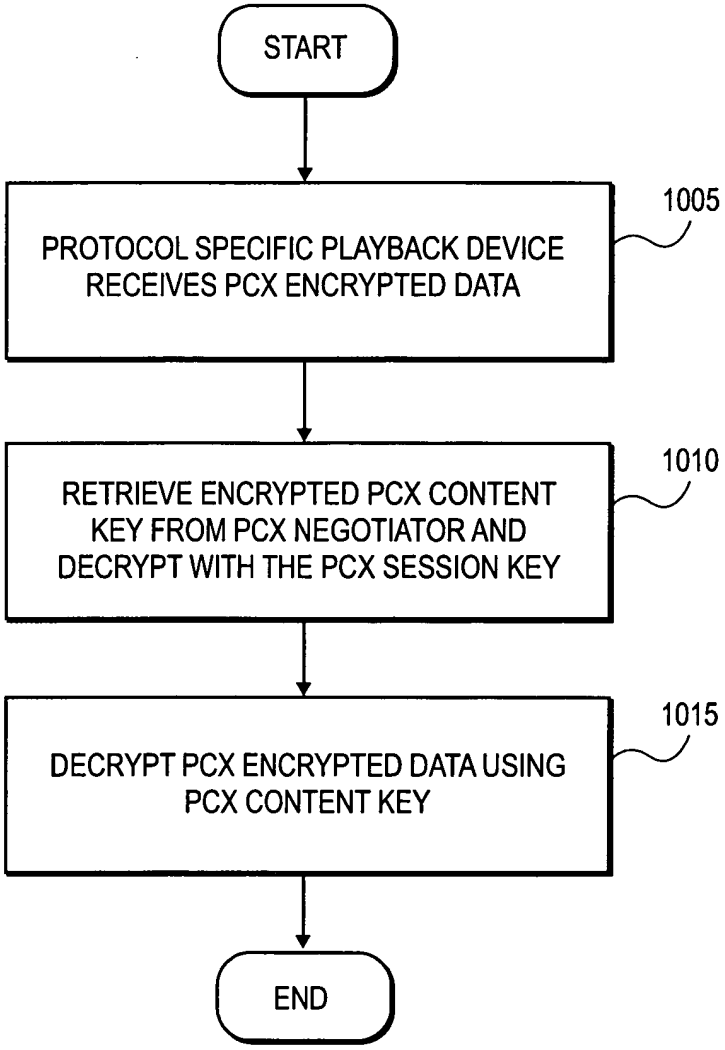

START
PROTOCOL SPECIFIC PLAYBACK DEVICE RECEIVES PCX ENCRYPTED DATA
1005
RETRIEVE ENCRYPTED PCX CONTENT KEY FROM PCX NEGOTIATOR AND DECRYPT WITH THE PCX SESSION KEY
1010
DECRYPT PCX ENCRYPTED DATA USING PCX CONTENT KEY
1015
END

FIG. 10

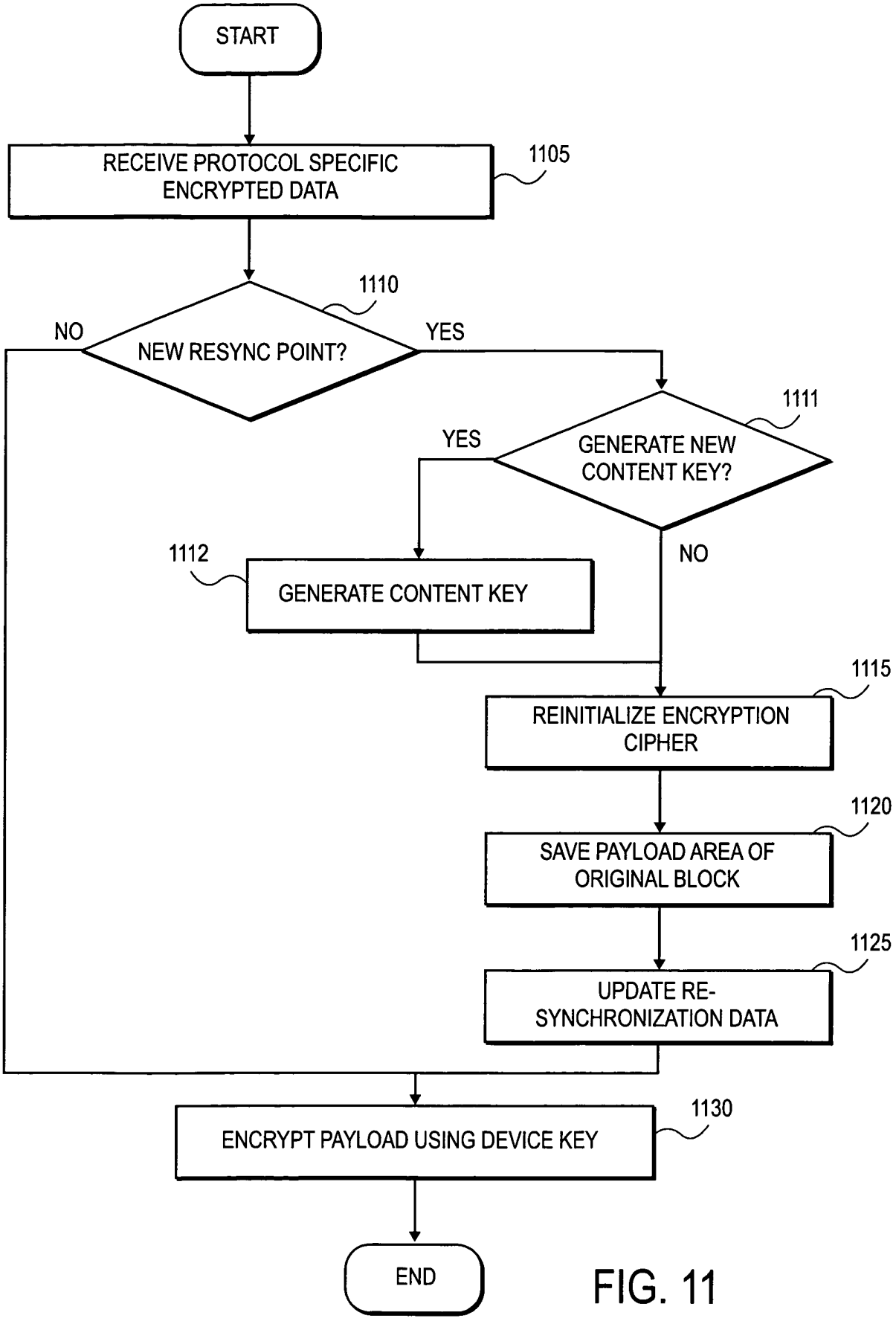

START
RECEIVE PROTOCOL SPECIFIC ENCRYPTED DATA
1105
1110
NEW RESYNC POINT?
NO
YES
1111
GENERATE NEW CONTENT KEY?
YES
NO
1112
GENERATE CONTENT KEY
1115
REINITIALIZE ENCRYPTION CIPHER
1120
SAVE PAYLOAD AREA OF ORIGINAL BLOCK
1125
UPDATE RE-SYNCHRONIZATION DATA
1130
ENCRYPT PAYLOAD USING DEVICE KEY
END

FIG. 11

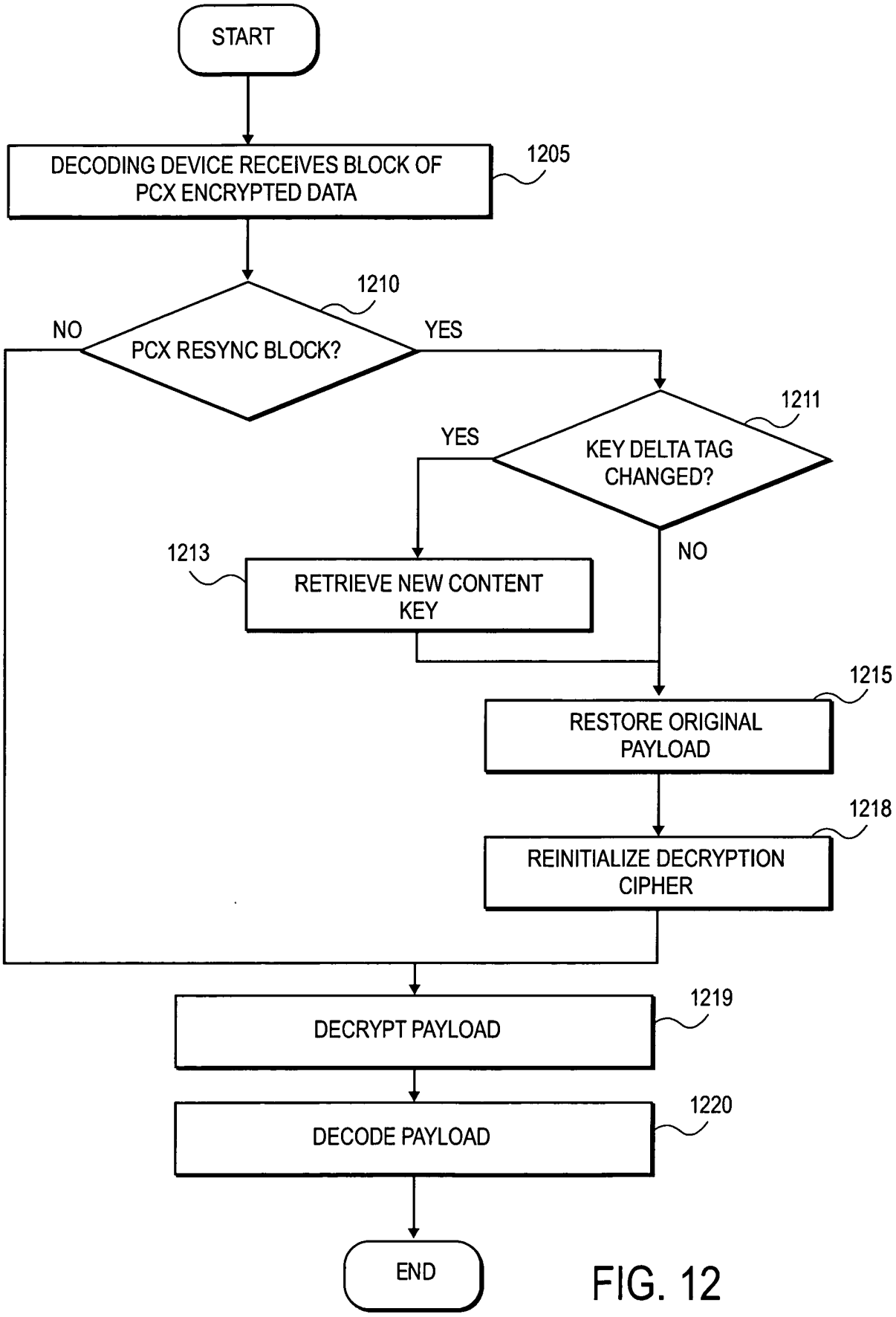

START
DECODING DEVICE RECEIVES BLOCK OF PCX ENCRYPTED DATA
1205
1210
PCX RESYNC BLOCK?
NO
YES
1211
KEY DELTA TAG CHANGED?
YES
NO
1213
RETRIEVE NEW CONTENT KEY
1215
RESTORE ORIGINAL PAYLOAD
1218
REINITIALIZE DECRYPTION CIPHER
1219
DECRYPT PAYLOAD
1220
DECODE PAYLOAD
END

FIG. 12

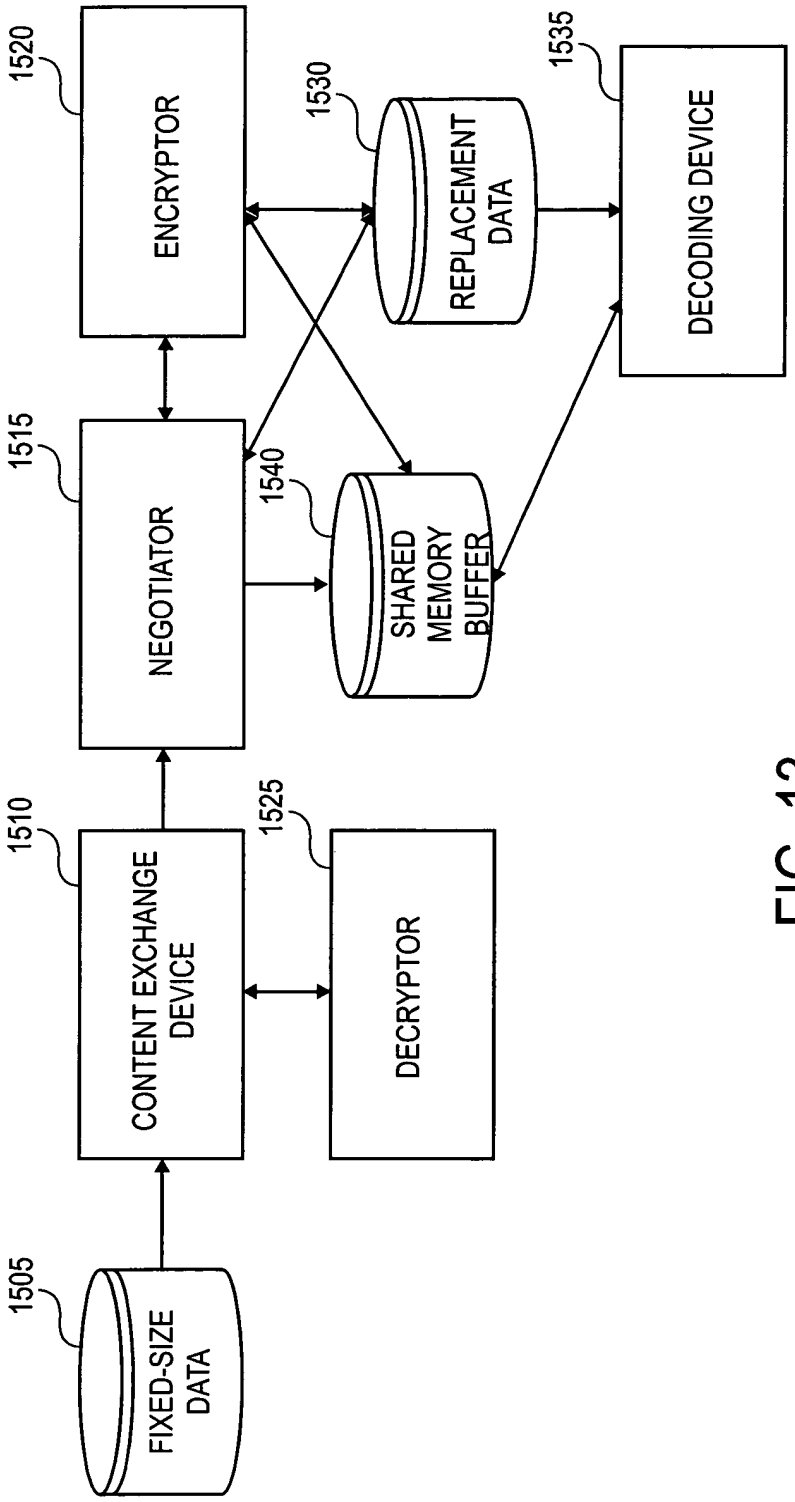

1520
ENCRYPTOR
1530
REPLACEMENT DATA
1535
DECODING DEVICE
1515
NEGOTIATOR
1540
SHARED MEMORY BUFFER
1510
CONTENT EXCHANGE DEVICE
1525
DECRYPTOR
1505
FIXED-SIZE DATA

FIG. 13

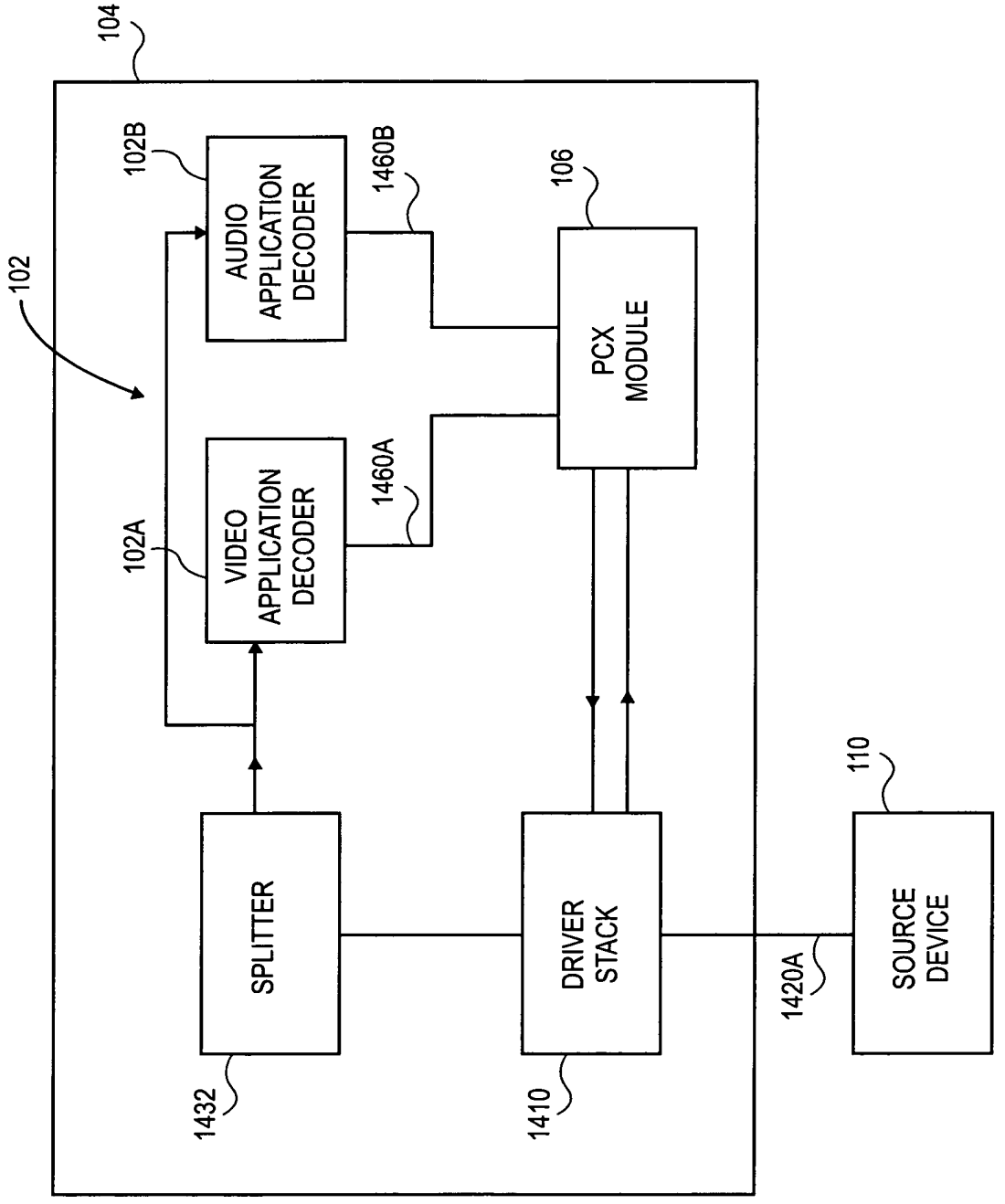

104
102B
AUDIO APPLICATION DECODER
1460B
106
PCX MODULE
102
102A
VIDEO APPLICATION DECODER
1460A
110
SPLITTER
DRIVER STACK
SOURCE DEVICE
1420A
1432
1410

FIG. 14

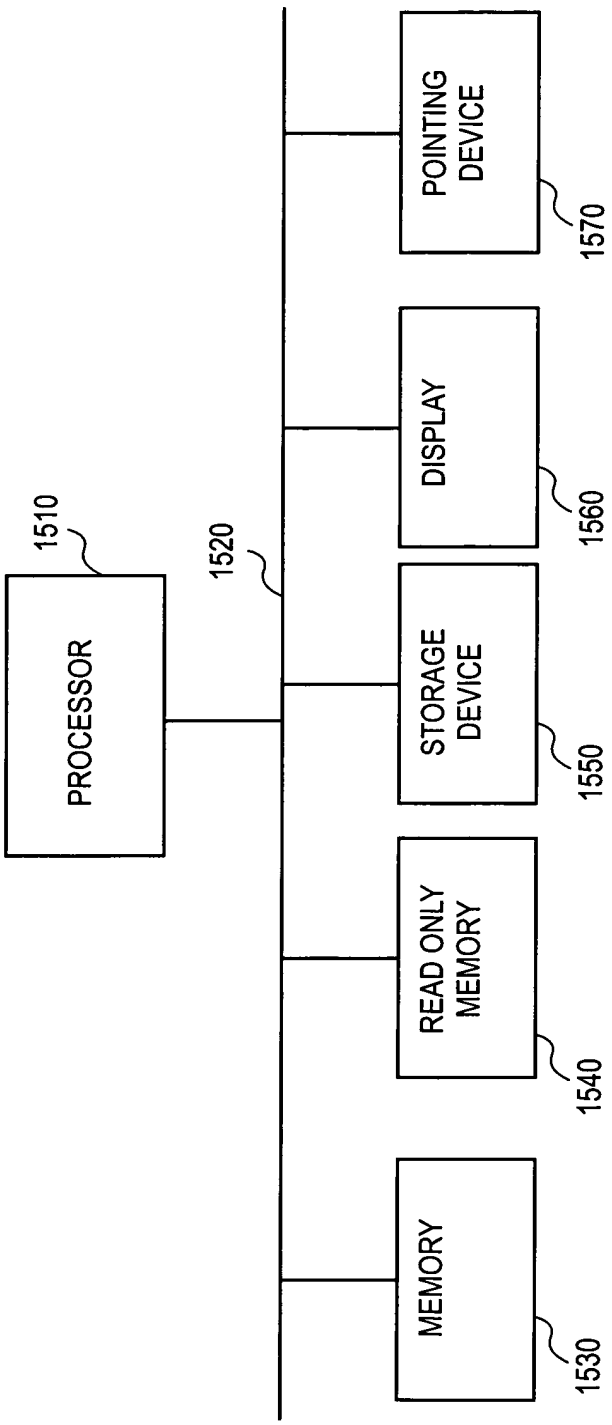

PROCESSOR
1510
1520
MEMORY
1530
READ ONLY MEMORY
1540
STORAGE DEVICE
1550
DISPLAY
1560
POINTING DEVICE
1570

FIG. 15

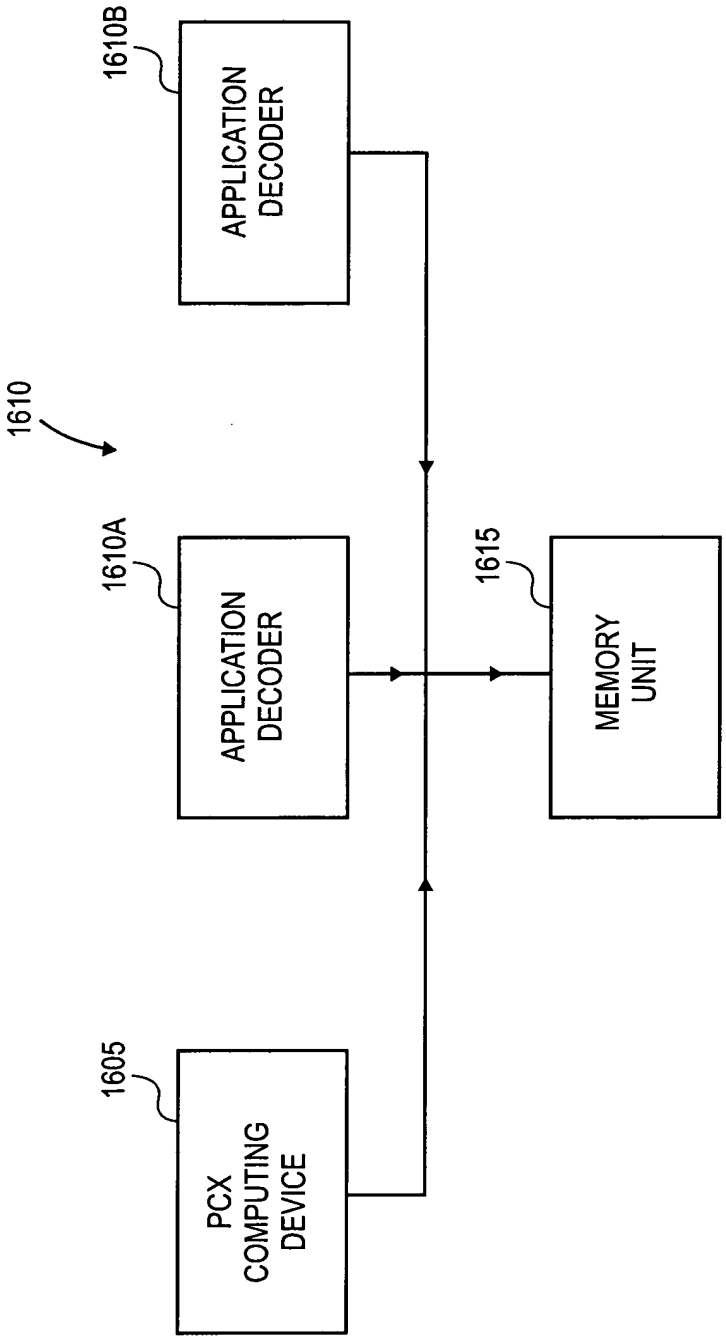

1610
1610B
APPLICATION DECODER
1610A
APPLICATION DECODER
1615
MEMORY UNIT
1605
PCX COMPUTING DEVICE

FIG. 16

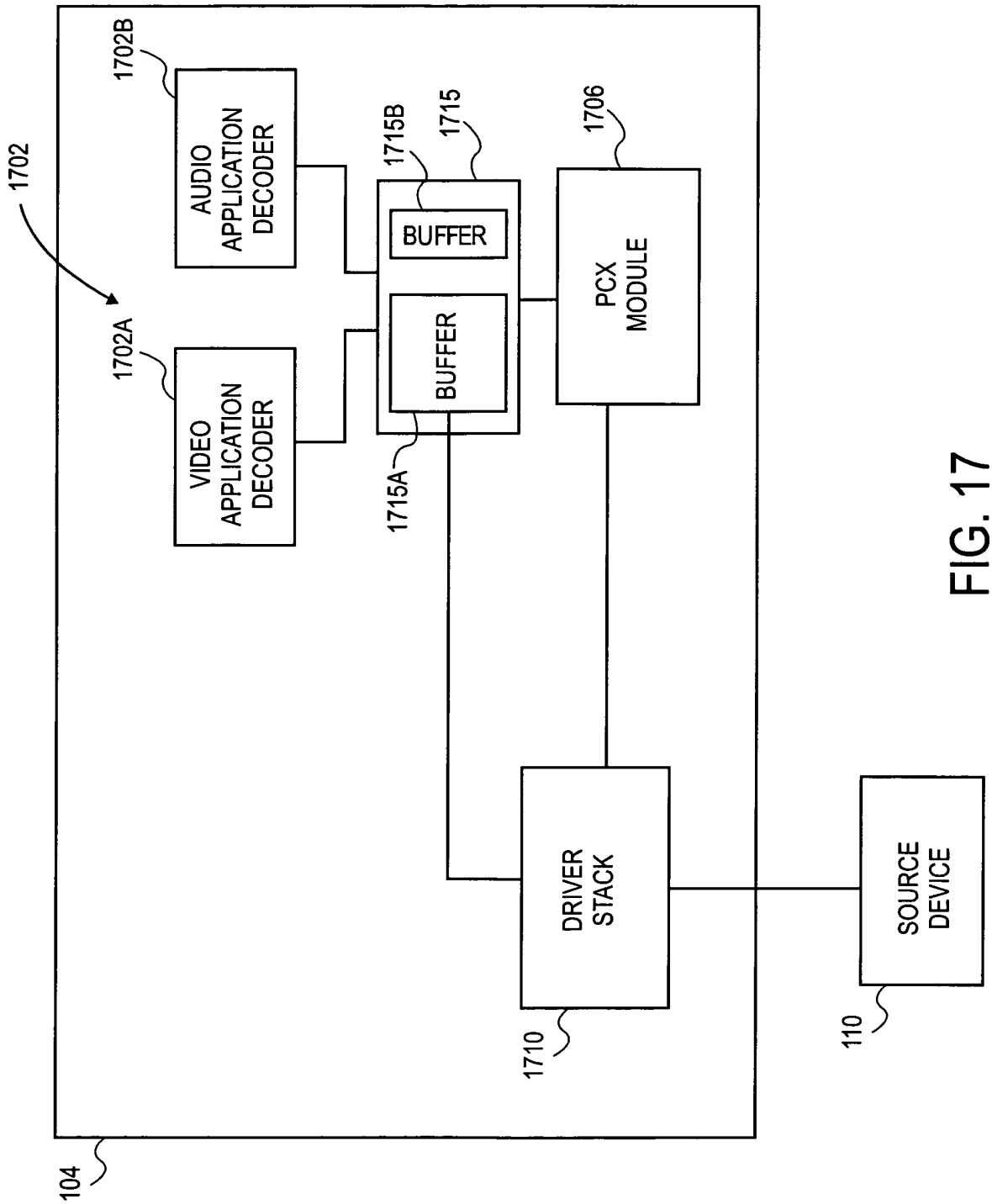

1702
1702B
AUDIO APPLICATION DECODER
1702A
VIDEO APPLICATION DECODER
1715B
1715
BUFFER
BUFFER
1715A
1706
PCX MODULE
DRIVER STACK
1710
SOURCE DEVICE
110
104

FIG. 17

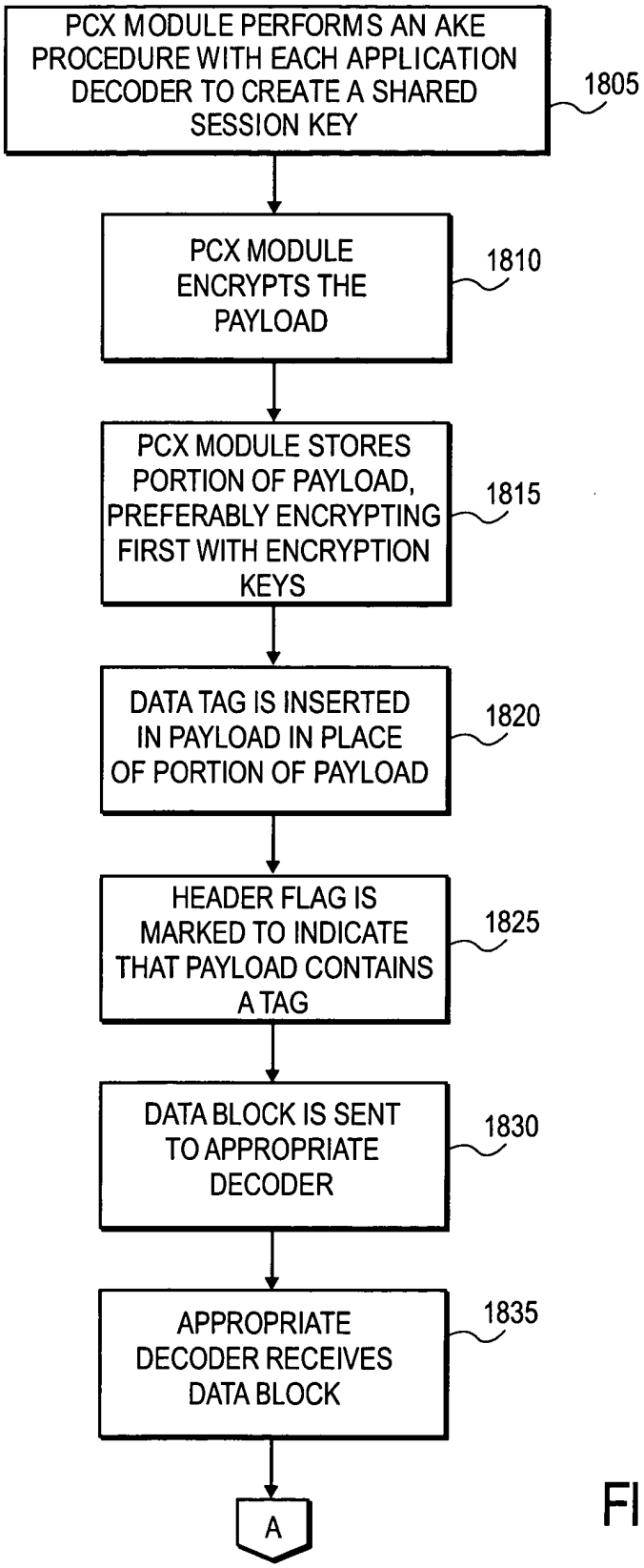

PCX MODULE PERFORMS AN AKE PROCEDURE WITH EACH APPLICATION DECODER TO CREATE A SHARED SESSION KEY
1805
PCX MODULE ENCRYPTS THE PAYLOAD
1810
PCX MODULE STORES PORTION OF PAYLOAD, PREFERABLY ENCRYPTING FIRST WITH ENCRYPTION KEYS
1815
DATA TAG IS INSERTED IN PAYLOAD IN PLACE OF PORTION OF PAYLOAD
1820
HEADER FLAG IS MARKED TO INDICATE THAT PAYLOAD CONTAINS A TAG
1825
DATA BLOCK IS SENT TO APPROPRIATE DECODER
1830
APPROPRIATE DECODER RECEIVES DATA BLOCK
1835
A

FIG. 18

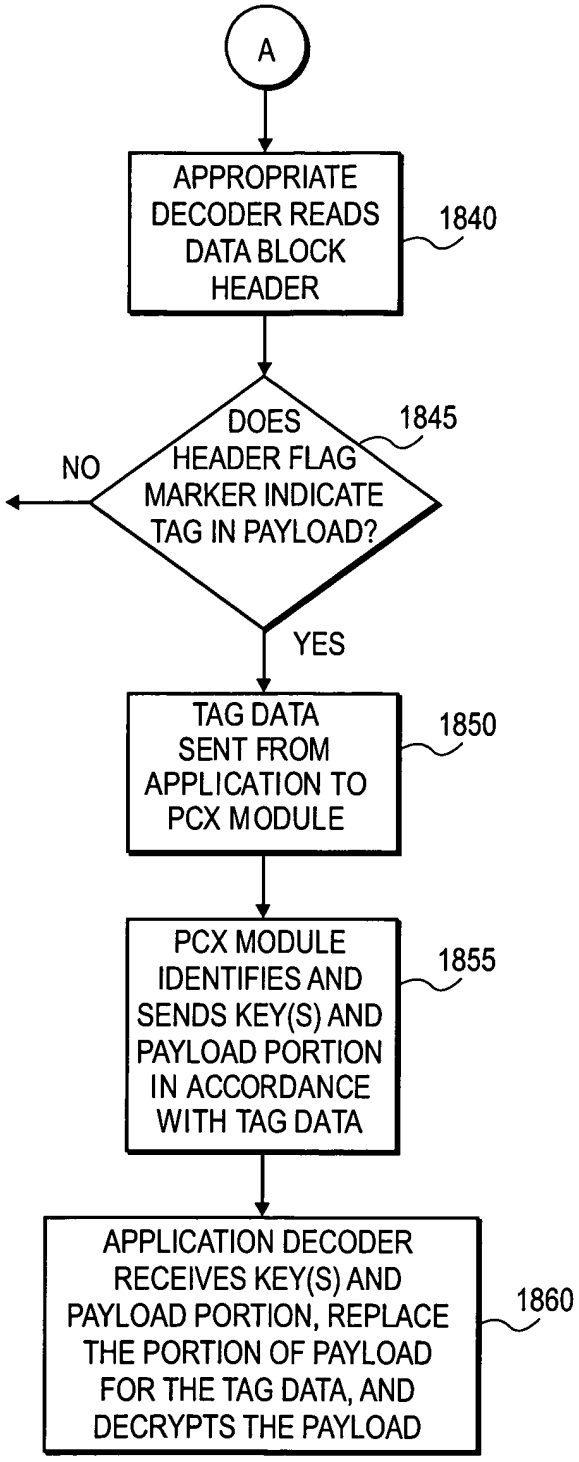

A
APPROPRIATE DECODER READS DATA BLOCK HEADER
1840
DOES HEADER FLAG MARKER INDICATE TAG IN PAYLOAD?
1845
NO
YES
TAG DATA SENT FROM APPLICATION TO PCX MODULE
1850
PCX MODULE IDENTIFIES AND SENDS KEY(S) AND PAYLOAD PORTION IN ACCORDANCE WITH TAG DATA
1855
APPLICATION DECODER RECEIVES KEY(S) AND PAYLOAD PORTION, REPLACE THE PORTION OF PAYLOAD FOR THE TAG DATA, AND DECRYPTS THE PAYLOAD
1860

FIG. 18 (CONT.)